Federal Chief Information Officers Council

July 6, 2000

Dear Colleague,

Over the past several months, the CIO Council Security, Privacy, and Critical Infrastructure Subcommittee has developed the attached Information Technology Security Assessment Framework. The Framework, a tool for agencies to assess the management of their IT security programs, is ready for your review and comment.

Three iterations of review/comment, comment resolution, and revision have resulted in this version of the document. The April 11 version, distributed at the CIO Council's Executive Committee, was revised based on comments received from nearly a dozen government and industry sources. During May of this year, several sessions were held to review comments and make appropriate changes to the draft document. The current draft represents the results of these reviews.

Our intent is for the CIO Council to review and comment on the attached draft by July 25, 2000. After your review, we plan to have one final open review of the document by industry and government representatives. This open review is tentatively planned for August 2000. After this open review, the document is to be published as Version 1. We request your comments on the current draft be sent to Dr. Fran Nielsen (fran.nielsen@nist.gov) as soon as possible, but not later than July 25, 2000.

Sincerely,

(SIGNED)

John M. Gilligan
CIO, Department of Energy
Co-Chair, Security, Privacy, Critical
Infrastructure Committee

Attachment

Attachment

Information Technology Security Assessment Framework

DRAFT – June 11, 2000

Prepared for

Security, Privacy, and Critical Infrastructure Committee

by

**National Institute of Standards and Technology (NIST)
Computer Security Division
Systems and Network Security Group**

Overview

Information is one of the most valuable assets of any organization. This sentiment is equally true with regard to Federal information systems. Protection of information, whether resident or in transit across networks, is vital and can be achieved only through effective management. Information security -- the protection of information from a wide range of threats in order to ensure business or mission continuity -- is a fundamental management responsibility.

Each Federal agency must provide an information security management infrastructure based on its mission and coupled with cost-effective IT security. In other words, rather than mandating a "one-size-fits-all" solution, agencies must consider their mission along with the value of their information and the impact of any potential risks. Vulnerabilities should be identified, reduced, eliminated or countered to the extent practicable and economically feasible. Decision-makers need to understand the factors that could negatively impact the mission so they can make informed judgments to minimize risk. Managing information risks, assessing vulnerabilities, and practicing due care are crucial.

The Information Technology (IT) Security Assessment Framework provides the means for Federal agencies to determine the current health of their security programs and, where necessary, to establish a target for improvement.

The Security Assessment Framework does not create new security requirements for agencies. Rather, as a tool to measure security programs, the Framework provides a vehicle for consistent and effective application of existing policy and guidance. Based on requirements of existing statute, OMB directives, GAO audit procedures, and NIST guidance, the Framework consists of a continuum of increased security capabilities and performance criteria to measure the effectiveness of them. These capabilities should be assessed throughout the risk management process and should be used on a continuing basis to determine the soundness of a security program.

The Framework can be used to seek assurance that responsibilities have been appropriately assigned and that everyone is aware of their responsibilities; that resources have been adequately allocated; and that risks are being appropriately addressed. The Framework will assess whether cost-effective information security oversight is in place.

The Framework comprises five levels to guide and prioritize agency efforts as well as to provide a basis to measure progress. At each level, more capability is expected. For example, response time is improved at higher levels of the continuum.

In developing the Framework, the Committee considered the concepts of the capability maturity model (CMM ®) of the Software Engineering Institute at Carnegie-Mellon University. The CMM is based on quality processes and methods used to develop software systems. The Framework is less qualitative but is equally focused on management, i.e., risk management. One difference between the CMM philosophy and that of the Framework is the notion that all systems should attain the highest level. This is not necessarily the case with the Security Assessment Framework. Agencies must consider their mission and the cost-effectiveness of security protection in determining what capability level to target and achieve. For some Federal information systems, level 3 may be entirely appropriate; other Federal systems, such as mission-critical systems, may need to strive for level 5.

Framework Description

The IT Security Assessment Framework identifies five levels of IT security program effectiveness. In partnership with those responsible for administering the IT system(s), it is the role of the mission owner to determine what level of effectiveness is appropriate. The Framework should be viewed as a continuum. As the figure below shows, it is expected that the majority of programs will be assessed at levels 2 through 4 with fewer agencies at either ends of the continuum. Level 3 may be entirely appropriate given the nature of the agency's mission and its understanding of risk. In fact, level 5 may not be the goal of every agency.

The Framework can be applied to assess an agency's overall program or it can be applied against a portion of that program. Example program portions are an IT security training program within an organization, an incident handling capability, a major application, or a general support system.

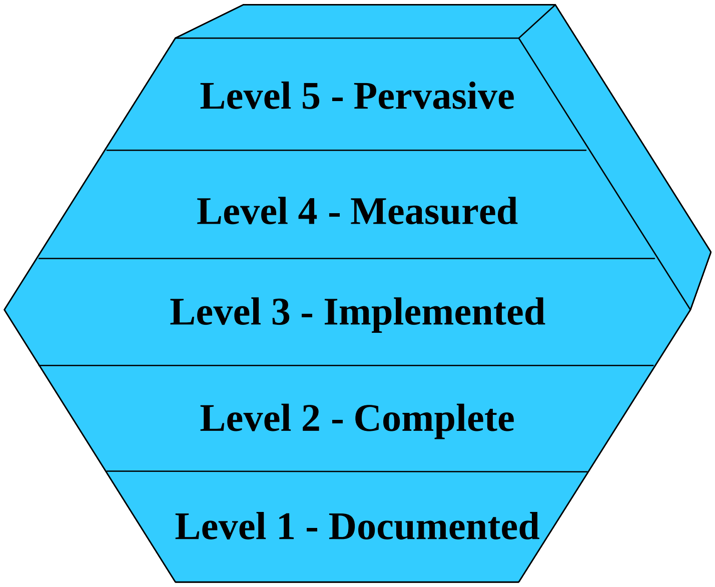


Figure 1 – Security Assessment Framework

Level 1 is a **documented**, but incomplete security program meeting most of the basic requirements of the Clinger-Cohen Act of 1996; the Paperwork Reduction Act of 1995; the Computer Security Act of 1987; OMB Circular A-130, *Management of Federal Information Resources*; GAO's *Federal Information System Control Audit Manual* (FISCAM); and NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)*. This program level encompasses most major agency components, e.g., bureaus and operating divisions, and includes approved system security plans for most agency general support systems and major applications.

Level 2 is a **complete** security program that meets all of the basic requirements of the statutory and policy authorities for level 1 and has been fully promulgated across all elements of an organization. This program level encompasses **all** major agency components, e.g., bureaus and operating divisions and includes approved security plans for **all** sites, critical systems and major applications.

Level 3 is a well-defined and **implemented** security program with detailed implementation procedures and corresponding security policies and mechanisms covering level 2 capability at each organizational element.

Level 4 is a **measurable** security program that has the capability to assess the effectiveness of implementation as well as to compare the cost of security feature(s) with a resulting decrease in security vulnerabilities and an ability to balance mission impact.

Level 5 is a **pervasive, continuously improving, and agile** security program that applies level 4 capabilities to increase security program cost-effectiveness. Level 5 can respond quickly, and in many cases in an automated fashion, to changes in threat, system characteristics or organization mission that effect overall organization risk.

An attempt to apply a specific security countermeasure to an immature security program will likely result in minimal, or even non-cost-effective, benefit. Combining a mature program with technically sound security countermeasures is the best way to obtain the security capability essential to protect the Federal infrastructure.

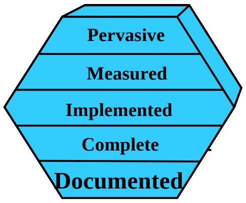
Levels 3 through 5 represent increased levels of security capabilities from the basic security management and processes contained in Levels 1 and 2. The capability of higher levels is built on the capability of the next lower level. The five levels will help guide and prioritize agency efforts and will provide a basis to measure progress.

Table 1 – Security Assessment Framework Overview

Level 1	***Documented Agency-wide Security Program*** Formally documented security program meeting most of the basic requirements of: • Clinger-Cohen Act of 1996 • Paperwork Reduction Act of 1995 • Computer Security Act of 1987 • OMB Circular A-130 • GAO/AIMD-12.19.6, FISCAM • NIST Special Publication 800-14, GSSP • Other appropriate policy and guidance (for example: OMB Memorandum 99-18 "Privacy Policies on Federal Web Sites")
Level 2	***Complete Agency-wide Security Program Including all Major Agency Components and Approved System Security Plans for All General Support Systems and Major Applications.*** • Formal and complete security program meeting all of the basic requirements of the authorities and guidance specified in Level 1 above. • Program has been fully promulgated across all elements of an organization.
Level 3	***Implemented Well-documented Agency-wide Security Program*** Complete security program including detailed, written procedures and corresponding security policies and mechanisms for implementing the program. Example procedures include: • Detailed system certification and accreditation procedures • Information Technology Security Training Implementation Plan with system-specific procedures • Detailed incident handling, reporting, and tracking procedures
Level 4	***Measured Well-documented Agency-wide Security Program*** Well-defined security program with ongoing, accurate measurement of the cost-effectiveness of the program. Actions such as: • Characterizing IT by degree of potential mission impact • Performing vulnerability assessments • Performing threat assessments • Positive reporting on identified vulnerabilities • Taking preventative and corrective actions to mitigate vulnerabilities

Level 5	***Pervasive, Continuously Improving, Agile, Well-documented Agency-wide Security Program*** Measured security program that applies and analyzes measurements to make decisions resulting in increased security capability and improved program cost-effectiveness. Responds quickly, and in many cases in an automated fashion, to changes in threat, system characteristics or organization mission that effect overall organization risk. Decisions include: • Improving security program plan and procedures • Improving or adding security countermeasures • Integrating and evolving security within IT architecture • Improving mission processes and risk management

Level 1 – Documented Security Program



- Level 1 - formally documented agency-wide security program covering agency headquarters and **most** major components (e.g., bureaus and operating divisions). The program includes approved systems security plans for **most** general support systems and major applications of the agency.
- Meets most of the basic requirements of Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, OMB Circular A-130, GSSP, and FISCAM.
- Most agencies at this level or higher

A level 1 IT security program consists of a formally documented program that establishes a continuing, agency-wide cycle of assessing risk, implements effective security policies including training, and promotes monitoring for program effectiveness. Such a program includes **most** major agency components, e.g., bureaus and operating divisions. Approved system security plans are in place for **most**, but not all, general support systems and major applications. Each system security plan identifies the particular agency program official responsible for security of the system. A documented security program plan is necessary to ensure adequate and cost effective organizational and system security controls. A sound agency-wide program that delineates the security management structure and clearly assigns security responsibilities, lays the foundation necessary to reliably measure progress and compliance and is essential for moving to the next level of assessment.

Level 1 Criteria

Level 1 criteria are abstracted directly from long-standing requirements found in statute, policy, and guidance on security, namely: the Computer Security Act of 1987; the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, OMB Circular A-130, *Management of Federal Information Resources*; GAO's *Federal Information System Control Audit Manual* (FISCAM); and NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)*. These documents provide descriptions of the recommended foundation for security planning and management efforts for Level 1 as well as all the remaining levels.

- Computer Security Act of 1987. This statute set the stage for protecting systems by codifying the requirement for Government-wide computer security planning and training.
- The Paperwork Reduction Act of 1995. The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
- The Clinger-Cohen Act of 1996. The Clinger-Cohen Act linked security to agency capital planning and budget

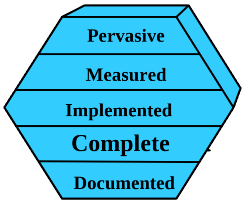
processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.

- OMB Circular A-130. A-130 establishes policy for Federal programs involving the collection, dissemination, publication, management, privacy, and safeguarding of information and information technology investments. Appendix III of this Circular establishes a minimum set of controls to be included in Federal information technology security programs and requires system security plans for all agency general support systems and major applications.
- FISCAM. The FISCAM methodology was originally developed to provide guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems. The manual is primarily designed for evaluating general and applications controls over financial information systems that support agency business operations. However, as the manual suggests, the methodology could be used to evaluate the general support system and major application controls in agency information systems, as called for in Government Auditing Standards.
- SP 800-14. NIST Special Publication 800-14 guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.

An agency's security program is assessed to be at level 1 if it is documented in a formally released Security Program Plan that meets the following criteria:

Criteria for Level 1	Y/N
a. Document security program plan. An agency-wide security program plan has been written that covers all major facilities and operations. The plan has been approved by key affected parties and covers security policies, risk management, vulnerability assessment, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources.	
b. Establish a security management structure (generally a "central security program office"). The security program comprises a security management structure with adequate independence, authority, and expertise. Information security manager(s) are appointed at an overall level and at appropriate subordinate levels.	
c. Assign information security responsibilities and expected behavior. Security responsibilities and expected behaviors are clearly defined for (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators.	
d. Periodically assess risks and vulnerabilities and monitor the computer security program's effectiveness. Risk management and vulnerability assessment activities are an integral part of the security program policy.	
e. System Security Plans. Approved and up-to-date system security plans are in place for most general support systems and major applications.	

Level 2 –Complete Security Program



- Level 2 – formal, complete, well-documented security program covering agency headquarters and **all** major components, e.g., bureaus and operating divisions.
- Meets **all** of the basic requirements of Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, OMB Circular A-130, GSSP, and FISCAM.

- Many agencies at this level or higher

A level 2 IT security program consists of a formally documented program plan establishing a continuing, agency-wide cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security program. The program includes **all** major agency components, e.g., bureaus and operating divisions. Approved system security plans are in place for **all** general support systems and major applications. Every plan identifies the particular agency program official responsible for security of the system. Well-documented security program plans are necessary to ensure adequate and cost effective organizational and system security controls. A sound agency-wide program that delineates the security management structure and clearly assigns security responsibilities, lays the foundation necessary to reliably measure progress and compliance and is essential for moving to the next level of assessment.

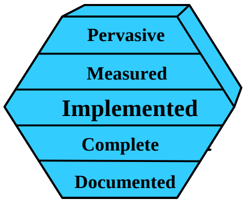
Level 2 Criteria

Level 2 criteria are essentially the same as the statutory and policy requirements found in level 1. The difference between level 1 and level 2 is in the **completeness** of addressing these requirements.

An agency's security program is assessed to be at level 2 if it covers **all** major agency components and if approved security plans exist for **all** general support systems and major applications. The criteria for level 1 are repeated here for completeness.

Criteria for Level 2	Y/N
a. Document security program plan. An entity-wide security program plan has been written that covers all major facilities and operations. The plan has been approved by key affected parties and covers security policies, risk management, vulnerability assessment, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources.	
b. Establish a security management structure (generally a "central security program office"). The security program comprises a security management structure with independence, authority, and expertise. Information security manager(s) are appointed at an overall level and at appropriate subordinate levels.	
c. Assign information security responsibilities and expected behavior. Security responsibilities and expected behaviors are clearly defined for (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators.	
d. Periodically assess risk and vulnerabilities and monitor the computer security program's effectiveness. Risk management activities are an integral part of the security program policy.	
e. System Security Plans. Approved and up-to-date system security plans are in place for **all** general support systems and major applications.	

Level 3 – Implemented Security Program



- Level 3 – implemented security program
- Includes detailed implementation procedures, such as:
  - Detailed system certification and accreditation procedures
  - Training plan with system-specific procedures
  - Detailed incident handling, reporting, and tracking procedures

- Some agencies have not achieved this level (i.e., formal plan exists, but implementation procedures are informal, incomplete, or lacking)

At level 3 the IT security program includes, in addition to a formal security program, detailed procedures for implementing it. The program also includes approved system security plans for all agency general support systems and major applications. Each security plan identifies the particular agency program official responsible for implementing the plan and many have formal implementing procedures. The addition of formal procedures represents a significant step in the effectiveness of the security program. As with the other levels of the Framework, a portion of the overall security program can be at level 3 while other aspects of an agency's security program are at other levels.

Formal implementing procedures promote the repeatability of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation.

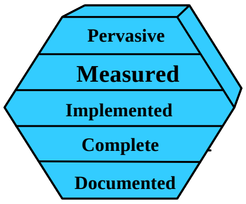
Level 3 Criteria

An agency's security program (or portion of a program) is assessed to be at least level 3 if, in addition to meeting all level 2 criteria, written implementation procedures are in effect and meet the following criteria:

Criteria for Level 3	Y/N
a. Make owners and users aware of security policies. Distribute security policies to all affected personnel, including system/application rules and expected behaviors. Require users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security.	
b. Review of security controls. Routinely use automated tools to monitor security. Establish policy on review of system logs, penetration testing, internal/external audits.	
c. Manage security throughout the life-cycle of the system. Consider security in each of the life-cycle phases: initiation, development/acquisition, implementation, operation, and disposal.	
d. Establish procedures for authorizing processing (certification and accreditation). Require management officials to formally authorize system operations and to manage risk.	
e. Implement effective security-related personnel policies. Accurately identify skill needs and include in job descriptions. Develop and implement termination and transfer procedures**.** Perform periodic reinvestigations. Ensure that employees receive adequate training and expertise to carry out security responsibilities. Document and monitor employee training and professional development.	
f. Implement physical and environmental security policies. Develop and implement procedures to protect the facility housing system resources, personnel in the facility, and the system resources.	
g. Implement security policy for computer support and operations. Develop and implement procedures to include: user support, executing new software, use of system utilities, license management, backups, and standardized log-on banner.	
h. Implement contingency planning policies. Require all major applications/general support systems to develop, test, and update contingency plans.	
i. Document system-specific security controls and operational procedures. Documentation for a system includes vendor-supplied hardware/software specifications, user manuals, testing procedures and results.	
j. Train employees on security requirements. Plan, implement, maintain, and evaluate an effective training and awareness program that is tailored for varying job functions.	

Criteria for Level 3	Y/N
k. Implement an incident response capability. Establish an incident response capability with characteristics suggested by the GSSP, e.g., use of virus identification software, an understanding of the constituency served, educated constituency that trusts the incident handling team, a means of prompt centralized reporting of incidents. Distribute vulnerability alerts and related remedial actions and implement needed patches promptly.	
l. Control access to system resources. Develop and implement identification and authentication policy and procedures for controlling access to system resources. Establish policy on user identifications, log-on attempts, passwords, access control lists, encryption, port protection devices, and firewalls.	
m. Implement audit trail policies. Develop procedures for audit trail review and analysis and for protecting the audit information from unauthorized access.	

Level 4 – Measured Security Program



- Level 4 – measured security program
- Contains capability to measure program cost-effectiveness
- Requires ability to:
  - Determine how IT insecurity can impact mission
  - Compare security cost with mission impact if not implemented
  - Relate security to resulting enhancement in mission capability
- Most agencies are likely below this level

An organization at level 4 is able to accurately determine the worth of a specific security capability. While this is essential to implementing a cost-effective program, organizations at lower levels may not be able to accurately determine the mission impact from a specific IT insecurity. Without this determination, it is unlikely that cost-effective protections will be implemented. Level 4 organizations understand information value and defend its damage, loss, and availability commensurate with its value. These organizations provide integrated security management. At lower levels, organizations perform some cost-effectiveness activities (for example, vulnerability, threat, and impact assessments), but they are only able to perform these in a rudimentary manner. Level 4 programs take an enterprise view of security when considering cost-effectiveness.

At level 4 the organization is able to make the determination that a specific security capability will result in mission capability at least equal to the cost of implementing the security measure. Additionally, the security measures are more likely to be viewed as enablers for efficient mission execution that otherwise would be too risky to undertake. Achieving level 4 requires the active involvement of the mission or business process owner in the security program.

An agency's security program is assessed to be at least level 4 if, in addition to meeting all level 3 criteria, the agency demonstrates the abilities:

- to conduct positive reporting on identified vulnerabilities and to take preventative and corrective actions on them; and

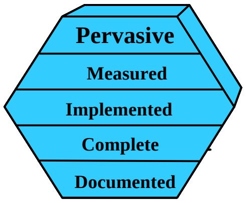
- to accurately determine:
  - the enhancement to mission capability provided by a given security measure and
  - the cost to implement that measure.

Level 4 Criteria

Criteria for Level 4	Y/N

Criteria for Level 4	**Y/N**
a. Understand value of information and mission impact of its loss, damage, or unavailability.	
b. Determine how IT insecurity can impact mission by measuring cost-effectiveness of security countermeasure and program impact.	
c. Compare security cost with mission impact if countermeasure is not implemented.	
d. Ensure that mission capability is at least equal to the cost of implementing a security measure.	
e. Exhibit proactive enterprise-wide security stance.	
f. Practice defense in depth – protect, detect, contain, and respond.	
g. View security measures as enablers to mission execution that might otherwise be too risky.	
h. Analyze metrics to evaluate effectiveness.	

Level 5 – Pervasive Security Program



- Level 5 – pervasive security program
- Importance of information security is an integral part of an agency’s organizational culture
- Decision-making that is based on knowledge related to cost-effectiveness balanced with mission impact
- Must be able to measure program, therefore level 5 builds on level 4
  - Few agencies at level 5

The consideration of information security is pervasive in the culture of a level 5 organization. A level 5 organization seeks to improve security cost-effectiveness and makes decisions based on knowledge about benefit and cost of implementing security. Decisions and actions include:

- Improving Security Program
- Improving Security Program Procedures
- Improving security countermeasures
- Adding security countermeasures
- Integrating security within IT architecture and evolving IT architecture
- Improving mission processes and risk management activities

Level 5 represents a significant increase in capability, by providing and exercising a range of options not available to many organizations. For organizations at a lower level, the only options typically available are to decide whether or not to implement or modify a given security countermeasure. The much more powerful options of modifying the IT architecture or the mission processes are frequently not available.

The level 5 organization is actively seeking to improve the cost-effectiveness of the security program. Security is an integral part of the organization’s mission and is seen as a necessary “cost of doing business.” This is accomplished by:

- understanding and portraying security as a mission enabler, by being able to relate the enhanced mission capability security provides,
- the mission owner being an active part of the security program, and
- having a full range of options available in deciding how to improve the mission capability with security being one

factor of the overall.

Organizations at a lower level may lack the ability to adequately measure the security program (level 4 capability). It is at level 5 that the understanding of mission costs is married with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures. As with level 4, achieving level 5 requires the direct involvement of the mission or business process owner.

Sound risk management **at all levels of the Framework** is expected. That is, organizations should apply the principle of selecting countermeasures that offer low cost of implementation while offering high risk mitigation versus selecting those with high cost of implementation and low risk mitigation.

Level 5 Criteria

Criteria for Level 5	**Y/N**
a. Apply cost-effective measures derived from level 4 in decision-making to achieve on-going improvement of security program.	
b. Demonstrate that information security is an integrated practice across the agency.	
c. Understand and manage security vulnerabilities.	
d. Continually re-evaluate threats and adapt to changing security environment.	
e. Identify additional or more cost-effective security alternatives as the need arises.	
f. Realize and show cost benefits of security.	
g. Encourage information security research activities.	

Future of the Framework

This version of the Framework primarily addresses security management issues. Essentially it provides a means for agencies to assess their compliance with long-standing basic requirements, such as those specified by the Computer Security Act of 1987; the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, OMB Circular A-130, *Management of Federal Information Resources*; GAO's *Federal Information System Control Audit Manual* (FISCAM); and NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)*. With the Framework in place, agencies will have a means to begin the assessment process to determine whether they are meeting these requirements.

The Framework is not a static document; it is a starting point. Revisions will focus on more granularity of existing criteria and on expanding and refining criteria for levels 4 and 5.

A number of issues remain open. The Framework appears to be primarily process-oriented. For now, it focuses little attention on whether the processes are effective. Determining effectiveness has several dimensions. Audits can demonstrate the effectiveness of agency security controls. As another dimension of effectiveness, it is assumed that an effectively designed process, properly implemented, will result in effective security. This may not necessarily be the case and is a more difficult measure to make. Then, there is the dimension of cost-effectiveness.

From another perspective, the Framework can be viewed as both an auditing tool and a management tool. Flexibility, contextual risk management, asset/mission-driven customization of improvement strategies and so on may be in conflict with statements about auditable process requirements. At some point, consideration of cost-effective information security oversight (i.e., the existence of the elements of a sound security program) and the successful protection of an organization's critical assets in a cost-effective manner (i.e., through asset-driven risk management) will lead to conflicting goals. Guidance will be needed on how to address these conflicts. This will be follow-on work.

Over time, the number and description of assessment levels may decrease. Perhaps, in the future, the differentiation among programs will be a compliant security program, a measured security program, and a pervasive, continuously improving security program.

Currently, companion work is needed at all levels to provide security checklists to help determine what cost-effective activities are being undertaken. Creation of the relevant checklists is a follow-on task.

Finally, another notable open issue relates to the assessment process itself. The initial goal of the Framework activity was to provide a tool for agencies to perform self-assessments or to be assessed by others. The frequency of assessments and other requirements on the process itself are not addressed in this version of the Framework.

Selected References

1. Clinger-Cohen Act of 1996
2. Paperwork Reduction Act of 1995
3. Computer Security Act of 1987
4. OMB Circular A-130, Management of Federal Information Resources
5. GAO/AIMD-12.19.6, Federal Information System Control Audit Manual (FISCAM)
6. GAO/AIMD-99-139, Information Security Risk Assessment Practices of Leading Organizations.
7. NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)

Acronyms

FISCAM	Federal Information System Control Audit Manual
GAO	Government Accounting Office
GSSP	Generally Accepted Principles and Practices for Security Information Technology Systems
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget